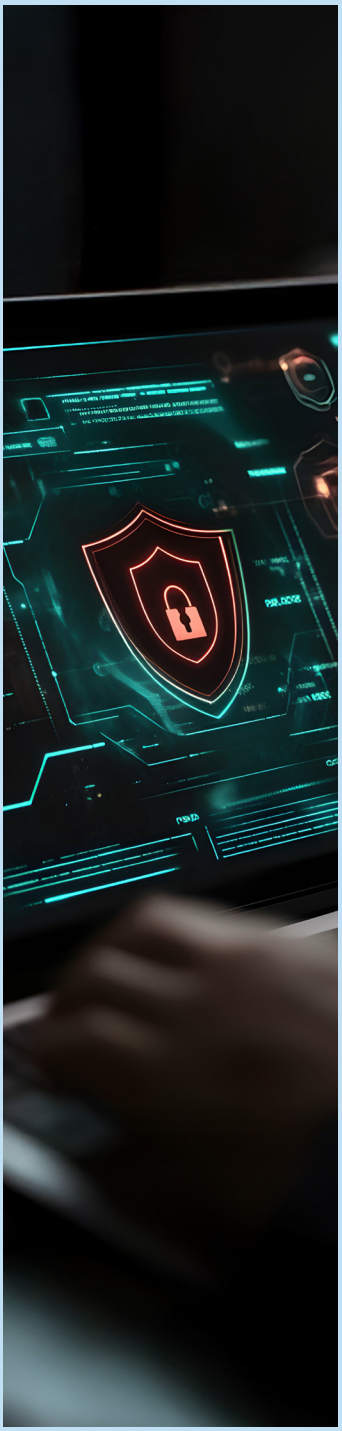
Infosys cobalt

VIEW POINT



FROM ENDPOINT CHAOS TO OPERATIONAL CONTROL

Infosys
Navigate your next

Introduction

Endpoints are now the operational edge of the enterprise - the point where security, compliance, and employee productivity converge. Yet many organizations continue to rely on fragmented tools for patching, asset management, and remote support, causing inefficiencies, higher overhead, and growing security risk.

Three shifts have made this an urgent leadership concern: hybrid work has expanded the endpoint perimeter; patch velocity and exposure windows have tightened; and tool sprawl has increased operating friction. Security risk grows when visibility is fragmented, manual operations do not scale, and user downtime becomes a direct productivity cost.

This Point of View makes the case for a unified endpoint management approach using ManageEngine Endpoint Central - examining the challenges, the proposed strategy, the solution's capabilities, and a clear path to implementation.

Challenges

Organizations managing endpoints through disconnected tools face four core challenges:

01

Fragmented Management Tools

Disconnected tools for patching, asset management, and remote support cause inefficiencies and higher overhead.

02

Lack of Endpoint Visibility

IT teams struggle to monitor device health, security, and compliance due to limited visibility, especially in remote work setups.

03

Manual Patching Delays

Manual patching processes slow down updates and increase vulnerabilities, posing serious security risks.

04

Security and Compliance Risks

Unmanaged endpoints and complex compliance requirements expose organizations to cyberattacks and regulatory challenges.

Proposed Strategy and Solution

The recommended response is to standardize on a unified endpoint platform - consolidating all endpoint management functions into a single operating model, automating routine tasks and policy enforcement, integrating with existing systems such as Active Directory, and enabling real-time monitoring and analytics for early issue detection.

ManageEngine Endpoint Central delivers on this strategy. It is a unified endpoint management platform that centralizes control, security, and automation across patch management, software deployment, asset and inventory management, remote support, mobile device management, and security and compliance -reducing tool sprawl and enabling a governed operating model for distributed endpoints.

Key Capabilities

Automated Patch Management:
Automatically updates operating systems and applications to prevent security vulnerabilities and maintain system integrity.

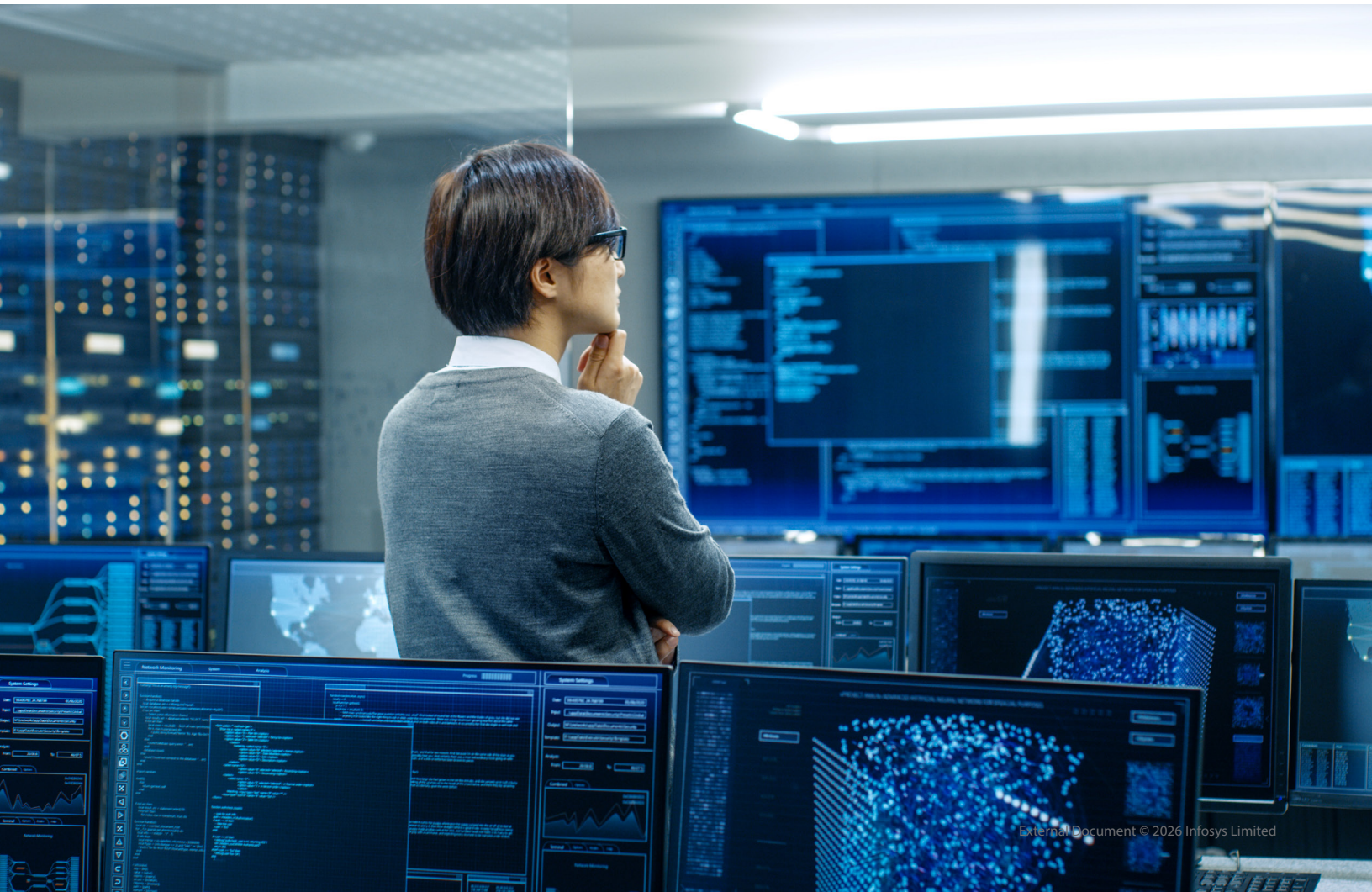
Efficient Software Deployment:
Distributes applications efficiently across multiple endpoints to reduce manual effort and improve consistency.

Remote Troubleshooting:
Provides real-time access to endpoints for quick issue resolution and minimal user disruption.

Comprehensive Asset Tracking:
Tracks all hardware and software assets to improve resource management and ensure compliance.

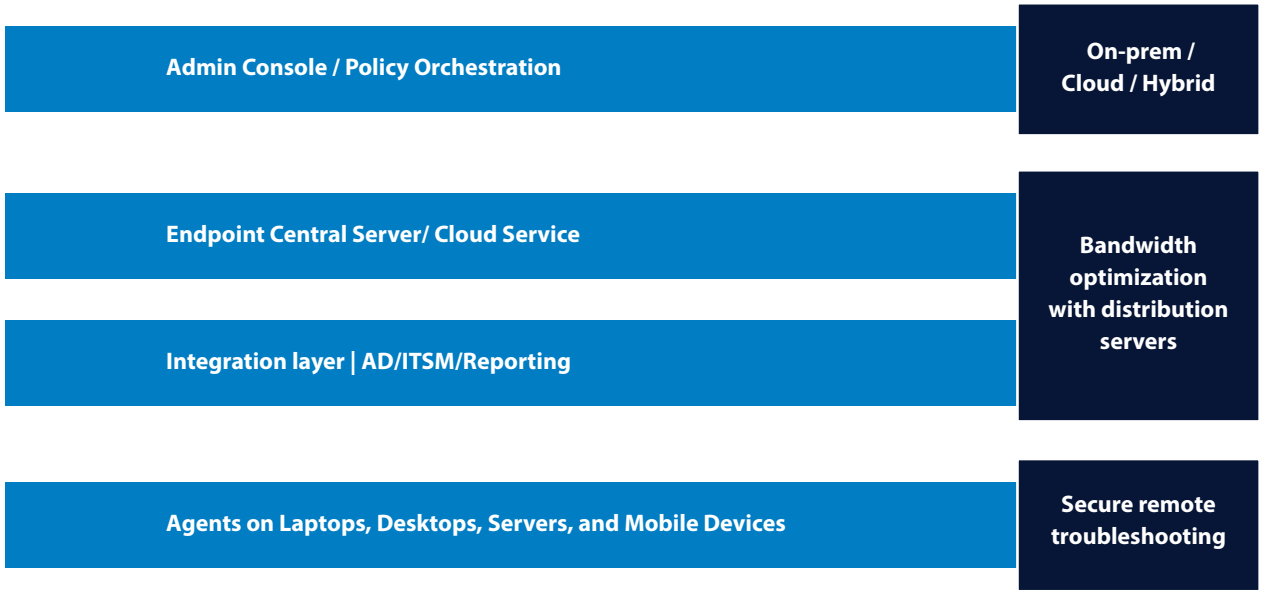
Mobile Device Management:
Provides visibility into hardware and software inventory and enables mobile device control to enhance compliance and security.

Enhanced Security Features:
Includes vulnerability management and data protection to improve the overall endpoint security posture.



Architecture

The platform is structured around an admin console for policy orchestration, an Endpoint Central server or cloud service, an integration layer connecting Active Directory, ITSM, and reporting tools, and agents deployed on laptops, desktops, servers, and mobile devices. It supports on-premises, cloud, and hybrid deployments with bandwidth optimization through distribution servers and secure remote troubleshooting. Integration with Active Directory enables seamless user and device synchronization.



Illustrative architecture view for executive discussion; deployment design should be finalized during the assessment phase.

Business Value

ManageEngine Endpoint Central delivers value across four executive priority areas:

Enhanced Security

Automated patching and continuous monitoring reduce cyber threat risks and ensure endpoint compliance.

Operational Efficiency

Automation of routine tasks like patching and software deployment reduces manual workload for IT teams.

Cost Optimization

Consolidating multiple tools into one platform lowers licensing and maintenance expenses significantly.

Compliance & Productivity

Detailed reporting supports regulatory compliance and improved visibility boosts productivity.

Measuring Success

Success should be measured against four KPIs established at baseline during the assessment phase:

Patch Compliance: Percentage of devices updated within set timeframes - above 95% indicates strong security.

Mean Time to Resolve (MTTR): Time taken to resolve endpoint issues - reductions reflect faster problem resolution.

Endpoint Visibility: All devices accounted for and managed effectively for comprehensive endpoint oversight.

Security Incident Monitoring: Number of security incidents - declines indicate improved protection.

Implementation Approach

A phased approach provides a structured path from pilot to scaled operating model:

Assess	Deploy	Stabilise	Optimise
Evaluate IT environment, identify endpoints, and analyse existing tools to define requirements and baseline.	Install endpoint server, deploy agents, and integrate with Active Directory for centralised management.	Configure patch management, security policies, and remote support while monitoring performance and resolving issues.	Enhance automation, build dashboards, and integrate with ITSM and SIEM tools for maximum efficiency.

Conclusion

Manage Engine Endpoint Central gives organizations a more structured way to manage, secure, and support endpoints from a single platform. By bringing together patching, asset visibility, remote support, automation, and compliance controls, it helps reduce tool sprawl, improve response times, and create a more consistent operating model for distributed work environments.

For enterprises looking to move from reactive endpoint support to proactive endpoint control, the next step should be focused discovery and pilot. This will help validate the platform against real user groups, baseline current gaps, and build a clear business case around security, efficiency, cost optimization, and user productivity.

About the Author

Venkateswara Rao Gorijavolu

Principal Technology Architect & Head of Unified Endpoint Management, Microsoft Practice, Infosys Limited

Venkateswara Rao Gorijavolu is a Principal Technology Architect and Head of Unified Endpoint Management Solutions at Infosys, with over 30 years of expertise in IT infrastructure design, implementation, and management across end-user computing environments He specializes in End User computing platforms consulting, program management, pre-sales, and IT service delivery and automations using AI. He leads EUC Transformation services globally, with a strong record in Digital Workplace solutioning, transformation strategy, and large-scale endpoint deployments.

For more information, contact askus@infosys.com

Infosys®
Navigate your next